

ATTORNEY'S DOCKET 064751.0315

86

WHAT IS CLAIMED IS:

5ub

15

25

30

1. Apparatus for multiplication of modular numbers, comprising:

a two-dimensional dependency array of cells, where each cell comprises:

a first full adder receiving a first input signal, a second input signal, and a clock signal,

a second full adder receiving an output of the 10 first full adder, a third input signal, and a clock signal;

a half adder receiving an output of the second full adder and a fourth input signal;

a first storage circuit coupled to the second full adder;

a second storage carcuit coupled to the half adder; and

a third storage circuit coupled to the half adder.

- 2. Apparatus for multiplication of modular numbers
 20 as in Claim 1 wherein the two-dimensional dependency
 array comprises a row by column configuration of cells.
 - 3. Apparatus for multiplication of modular numbers as in Claim 1 wherein the two-dimensional dependency array comprises groups of two dependency graph cells coupled together to add within one pair of cells product terms of equal weight.
 - 4. Apparatus for multiplication of modular numbers as in Claim 1 further comprising a binary number reduction circuit sequentially coupled to the output of the two-dimensional dependency array of cells.

5

10

15

20



ATTORNEY'S DOCKET 064751.0315

87

5.	Apparatus	for	multipl/cation	of	modular
numbers,	comprising:		/		

a two-dimensional dependency array of cells, wherein each cell comprises:

a first full adder receiving a first input signal, a second input signal, and a clock signal;

a second full adder receiving a third input signal, a fourth input signal, and a clock signal;

a third full adder receiving an output of the second full adder, a fifth input signal, and an output of the first full adder, and providing an output signal;

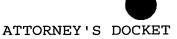
a fourth full adder receiving an input from the first full adder, an input from the second full adder and providing an output to the first full adder;

a first storage circuit coupled between the second full adder and the third full adder;

a second storage circuit coupled between the fourth full adder and the first full adder; and

a third storage circuit in a feedback loop coupled to the fourth full adder.

- 6. Apparatus for multiplication of modular numbers as in Claim 5 further comprising a reduction circuit coupled to the two-dimensional dependency array and sequentially receiving signals therefrom.
- 7. Apparatus for multiplication of modular numbers as in Claim 6 wherein said reduction circuit comprises a row by column array of cells.



064751.0315

5



PATENT APPLICATION

88

8. Apparatus for multiplication of modular numbers as in Claim 6 wherein the two-dimensional dependency array of cells comprises a binary multiplier, and the reduction circuit comprises concurrent reduction sequentially receiving signals from the binary multiplier.

15

20



ATTORNEY'S DOCKET 064751.0315

89

- 9. Apparatus for multiplication of modular numbers, comprising:
- a serial array of interconnected cells each comprising:
- a first full adder receiving a first input signal, a second input signal, and a clock signal;
 - a first storage circuit coupled in a feedback loop between an output of the first full adder and an input thereto;
- a second storage circuit receiving the first input signal and providing an output signal;
 - a third storage circuit coupled to the first full adder and the second storage circuit and providing an output to the adjacent cell.
 - 10. Apparatus for multiplication of modular numbers as in Claim 9 wherein adjacent cells are interconnected in a serial adder configuration.
 - 11. Apparatus for multiplication of modular numbers as in Claim 8 further comprising a concurrent reduction cell, and wherein the concurrent reduction cell comprises:
 - a first full adder receiving a first input signal, a second input signal, and a clock signal;
- a second full adder receiving an output of the first full adder, a third input signal, and a clock signal;
 - a first storage circuit coupled to an output of the first full adder and an input thereto;
 - a second storage circuit coupled to an output of the second full adder and an input thereto;
- a third storage circuit coupled to an output of the first full adder and providing an output; and



90

- a fourth storage circuit coupled to the second storage circuit and the second full adder.
- 12. Apparatus for multiplication of modular numbers as in Claim 10 further comprising:
- a first serial shift register having as an output the first signal coupled to the full adder;
- a second serial shift register providing the second input to the first full adder of the first cell in the serial configuration; and
- a third serial shift register serially receiving an output from the third storage circuit of the last serial adder in the serial configuration and providing a parallel output signal.

addeil

5